

2018年2月26日

個人向けインターネット・モバイルバンキングの不正送金にご注意ください

インターネットバンキングにおいて、不正送金被害が増加しております。

お客さまにおかれましてはくりょうしん>インターネット・モバイルバンキングをより安全にご利用いただくため、以下のセキュリティ対策を行なっていただくようお願いいたします。

記

1. セキュリティ対策ソフトの最新化と定期的なチェック

パソコンには必ずセキュリティソフトを導入し、最新版へのアップデートをお願いします。また、ウイルスに感染していないことを定期的を確認してください。

2. パスワード等の定期的な変更

パスワード等は、必ず定期的に変更を行ってください。また、漏えい防止のため、同一パスワードの他のサービスでの使い回しは行わないようにご注意ください。

3. OSやブラウザ等の最新化

OSやブラウザ等、パソコンにインストールされている各種ソフトウェアには、適宜、最新の修正プログラムを適用してください。

4. 振込限度額の確認

振込限度額は必要最低限に設定してください。

5. ソフトウェアキーボードのご利用

ID・パスワード等のウイルスによる漏えいを防止するため、入力欄への直接入力を避け、ソフトウェアキーボードを利用されることを推奨します。

6. 不審なメールは絶対に開かない

ウイルスに感染する危険性があります。心あたりのないメールに記載されているURLのクリックや添付ファイルの開封などは行わないでください。

7. 推奨するセキュリティ対策（無料）

- ・「PhishWall（フィッシュウォール）プレミアム」の利用

お客さまのPCがMITB攻撃型ウイルスに感染していないかをチェックし、感染の徴候を発見した場合に、警告画面で情報の入力をブロックします。また、ウイルスを無効化する機能が搭載されています。

詳しくは[「PhishWallプレミアムの説明」](#)をご確認ください。

- ・「ワンタイムパスワード」の利用

最大有効期限が1分の可変パスワードです。携帯電話もしくはスマートフォンを利用してランダムに作成されたパスワードを通知します。表示されているパスワードを入力することでご本人さまの確認を行ないます。

[ワンタイムパスワード詳しい説明はこちら](#)

8. メール通知パスワードの利用（ワンタイムパスワードとの併用不可）

ログインする都度、あらかじめ指定されたメールアドレスにランダムに作成した可変パスワードを記載したメールが送信され、そのパスワードを入力することでご本人さまの確認を行ないます。

上記に関するご質問・お問い合わせや、万一不正アクセスによる被害を受けられた場合は、経営管理本部（TEL095-861-4161）または最寄りのりょうしん各営業店までご連絡ください。

以上